Application No. 09/893,736

Atty. Docket No. 042390.P11033
Examiner: Taghi T. Arani
TC/A.U. 2131

REMARKS

Claims 1-16, 19-23, and 25-28 are pending. Claims 17-18, 24, and 29-34 were previously cancelled.

Applicant's note with appreciation the apparent withdrawal of the rejections under 35 U.S.C. § 112, second paragraph. The front page of the current Office Action indicates that the Action in non-final. Also PAIR has this Office Action docketed as non-final. However, the last page of the Office Action suggests that it is final since applicant's previous amendments necessitated a new ground of rejection. However, the previous amendment was to clarify 112, second paragraph matters only and the there does not appear to be a new ground of rejection, although the 112, second paragraph rejection has been overcome. Therefore, it is believed that this Action is non-final.

Claims 1, 3-7, 9-16, 19-23, 25-26, and 27 stand rejected under 35 U.S.C. § 103 as being unpatentable over D. Harkins "The Internet Key Exchange" (hereinafter IKE) in view of Maughan (Internet Security Association and Key Management Protocol" (hereinafter ISAKMP), both of record.

Claims 2, 8, 26, and 28 stand rejected under 35 U.S.C. § 103(a) as

being unpatentable over IKE and D. Dukes et al., "ISAKMP Configuration

Model", The Internet- Draft, March 2000, further in view of Y. Dylan et al.,

"IKE Base Mode", Internet-Draft, January 2000.

These rejections are respectfully traversed based on the following

discussion.

Briefly, embodiments of the present invention offer a way to

dynamically configure a secure tunnel between a client (first peer) and a

remote Gateway (second peer) over a network, such as the Internet. During a

Phase 1 negotiation, the first peer offers a plurality of security configuration

proposals. The second peer may then select one of these security configuration

proposals and send its choice back to the first peer.

All of the references have been previously discussed. The heart of the

issue appears to be Maughan (Internet Security Association and Key

Management Protocol" (hereinafter ISAKMP) which the Examiner relies on to

teach "offering more secure proposals before less secure proposals". The

previous discussion of the other references is incorporated herein by reference

for completeness of response and not resubmitted herein for clarity.

In the Examiner's response to the previous arguments, the examiner

asserts that ISAKMP statement that "in decreasing order of preference that a

system considers acceptable to protect traffic under a given situation" suggests

ordering from a higher level of security to a lower level of security, as claimed.

It is respectfully submitted that this "suggestion" to which the

Examiner refers comes only from Applicant's own specification. Offering a

list in decreasing order of preference does not suggest offering "more secure

proposals before less secure proposals" as claimed.

The examiner cannot rely on the applicant's own disclosure and

combine the references based on this hindsight. To support a conclusion of

prima facie obviousness, either the references must expressly or impliedly

suggest the claimed combination or the examiner must present a convincing

line of reasoning as to why the person of ordinary skill in the art would have

found the claimed invention obvious in light of the teachings of the references.

Ex Parte Clapp, 227 USPQ 972. The mere fact that the prior art could be

modified as proposed by the examiner, absent a motivation to do so provided

by the reference, does not support the rejection. In re Gordon, 221 USPQ

1125, 1127; In re Deminski, 230 USPQ 313, 315.

Applicants submit that "preference" as used by ISKMP does not

suggest "more to less secure" since a particular protection suite may be

"preferred" for any number of reasons including, complexity, overhead, etc. in

a given traffic situation. Further a protection "suite" does not commonly

Àpplication No. 09/893,736

Atty. Docket No. 042390.P11033
Examiner: Taghi T. Arani
TC/A.U. 2131

denote security protocols, but rather software bundles or software suite used for things such as virus protection, spam protection, URL filtering, etc. Indeed , this only "suggestion" that the ISKMP use of the term "preference" suggests "more to less secure protocols" is found in Applicant's own patent application.

Nothing in the ISKMP reference, alone or in combination with the other art of record teaches or suggests ordering "security configuration proposal having a higher level of security is offered before a security configuration proposal having a lesser level of security" as claimed. The teachings of ISKMP are ambiguous on this topic at best. Deficiencies in the factual basis needed to support a rejection under 35 U.S.C. §103 cannot be supplied by resorting to speculation or unsupported generalities.

In view of the foregoing, it requested that the application be reconsidered, that claims 1-16, 19-23, and 25-28 be allowed and that the application be passed to issue. Please charge any shortages and credit any overcharges to our Deposit Account number 50-0221.

Should the examiner find the application to be other than in condition for

allowance, the examiner is requested to contact the undersigned at the local

telephone number listed below to discuss any other changes deemed necessary

in a telephonic interview.

                                        Respectfully submitted,

                                        /Kevin A. Reif/

                                        Kevin A. Reif
                                        Reg. No. 36,381

INTEL
LF1-102
4050 Lafayette Center Drive
Chantilly, Virginia 20151
(703) 633-6834